

Making the NextGen Vision a Reality

# Joint Planning and Development Office

## Security Annex Concept of Operations for the Next Generation Air Transportation System

Version 2.0

13 June 2007



# NEXTGEN

Next Generation Air Transportation System

Report Documentation Page			Form Approved OMB No. 0704-0188		
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE <b>13 JUN 2007</b>		2. REPORT TYPE		3. DATES COVERED <b>00-00-2007 to 00-00-2007</b>	
4. TITLE AND SUBTITLE <b>Security Annex Concept of Operations for the Next Generation Air Transportation System Version 2.0</b>				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Joint Planning and Development Office, Next Generation Air Transportation System (NextGen), 1500 K Street NW Suite 500, Washington, DC, 20005</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>Same as Report (SAR)</b>	18. NUMBER OF PAGES <b>51</b>	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			





## ANNEX: LAYERED, ADAPTIVE SECURITY OPERATIONAL CONCEPT FOR NEXTGEN

### PREFACE

The Joint Planning and Development Office (JPDO) is developing a concept of operations (ConOps) for the Next Generation Air Transportation System (NextGen). The final version of the ConOps will provide an overall and integrated view of NextGen operations in the 2025 timeframe, including key transformations from today's operations. The overall document also identifies key research and policy issues that need resolution to achieve national goals for air transportation. The development of the ConOps is an iterative and evolutionary process that will progress using input and feedback from the aviation community.

This document provides the aviation community with a preview of the NextGen ConOps and receive their comments for improvements. Details of the JPDO comment and review process can be found at the Tech Hanger at [www.jpdo.aero](http://www.jpdo.aero). The full version of this document will include accepted comments for the NextGen concepts related to the following;

- Airport operations and mission support
- Air traffic management planning and mission support services
- Flight operations planning and mission support services
- Layered adaptive security services
- Network-enabled infrastructure services
- Shared situational awareness services
- Safety management services
- Environmental management services
- Compliance, regulation, and harmonization services.

Often, this document presents “aggressive” concepts that have not been validated but are envisioned as attainable goals to maximize benefits and flexibility for NextGen users of 2025 and beyond. Many potential futures are possible, and much will depend on the insights gained by the evolution and increasing specificity of the ConOps. Comments to refine these research issues are requested.

The attached document, which is the full version of Chapter 6 in the initial NextGen ConOps plan, describes the entire concept of layered adaptive security at the same high level as other chapters.



## TABLE OF CONTENTS

<b>PREFACE.....</b>	<b>1</b>
<b>1 INTRODUCTION.....</b>	<b>1</b>
1.1 OVERVIEW .....	1
1.2 NEXTGEN SECURITY MANAGEMENT AND COLLABORATIVE FRAMEWORK .....	2
1.3 NEXTGEN SECURITY OPERATIONAL IMPROVEMENTS SUMMARY .....	3
<b>2 INTEGRATED RISK MANAGEMENT.....</b>	<b>5</b>
2.1 RISK MANAGEMENT PROCESS .....	6
2.2 SECURITY RISK MANAGEMENT.....	6
2.2.1 IRM—Secure People .....	7
2.2.2 IRM—Secure Airports.....	7
2.2.3 IRM—Secure Checked Baggage .....	8
2.2.4 IRM—Secure Cargo/Mail.....	8
2.2.5 IRM—Secure Airspace.....	9
2.2.6 IRM—Secure Aircraft .....	10
2.3 NEI-ENABLED INTEGRATED RISK MANAGEMENT COLLABORATION ENVIRONMENT .....	11
2.4 RISK MANAGEMENT STRATEGY MONITORING AND FOLLOW-UP.....	12
<b>3 SECURE PEOPLE .....</b>	<b>13</b>
3.1 INTEGRATED RISK MANAGEMENT .....	13
3.2 AUTHENTICATION AND CREDENTIALING .....	13
3.2.1 Credentialing.....	14
3.2.2 Passenger Authentication.....	14
3.2.3 Aviation Industry Worker Authentication .....	15
3.3 CHECKPOINT PERSON SCREENING .....	15
3.4 CHECK POINT BAGGAGE SCREENING.....	16
3.5 CONTINUOUS SURVEILLANCE AT CHECKPOINT/ACCESS SITES .....	17
3.6 GLOBAL HARMONIZATION.....	18
<b>4 SECURE AIRPORTS.....</b>	<b>19</b>
4.1 IRM—SECURE AIRPORT .....	19
4.2 AIRPORT FACILITIES .....	20
4.2.1 Commercial (Passenger/Cargo) Airports.....	20
4.2.2 Remote Terminal Security Screening .....	20
4.2.3 General Aviation Airports.....	20
4.2.4 Commercial Spaceports .....	21
4.3 AIRSIDE .....	21
4.3.1 AOA/SIDA .....	21
4.3.2 Terminal Perimeter .....	21
4.3.3 Terminal Airspace Security .....	22
4.4 LANDSIDE .....	22
4.4.1 Airport Public and Commercial Roadways and Parking Lots .....	22
4.4.2 Terminal Departures Curb .....	22
4.4.3 Terminal Entry Portal .....	23
4.4.4 Airline Ticketing Kiosk/Counter .....	23
4.4.5 Security Checkpoint.....	23

4.4.6	Sterile Concourse .....	23
4.4.7	International Arrival/Customs .....	23
4.4.8	Airport Concessions, Food, and Beverage Security .....	24
4.5	AIRPORT SECURITY CONTROL CENTER.....	24
4.6	EMERGENCY RESPONSE AND RECOVERY .....	24
<b>5</b>	<b>SECURE CHECKED BAGGAGE.....</b>	<b>25</b>
5.1	INTEGRATED RISK MANAGEMENT .....	25
5.2	CHECKED BAGGAGE SCREENING .....	26
5.2.1	Screening.....	26
5.2.2	Alarm Resolution Screening .....	26
5.2.3	Threat Object Disposal .....	27
5.3	CHECKED BAGGAGE SCREENING INSTALLATIONS .....	27
5.3.1	In-Line Baggage Screening.....	27
5.3.2	Nonintegrated and Standalone Baggage Screening .....	28
5.3.3	Deployable Baggage Screening Operations.....	28
5.4	GLOBAL HARMONIZATION.....	28
<b>6</b>	<b>SECURE CARGO AND MAIL.....</b>	<b>29</b>
6.1	INTEGRATED RISK MANAGEMENT .....	30
6.2	SHIPPER CREDENTIALING.....	30
6.3	SCREENING AND INSPECTION .....	31
6.4	ALARM RESOLUTION .....	31
6.5	SURFACE TRANSPORTATION SECURITY OF SCREENED CARGO.....	32
6.6	HARDENED DOORS AND BARRIERS ON ALL CARGO AIRCRAFT .....	32
6.7	SECURITY TRAINING FOR ALL CARGO FLIGHT CREW AND STAFF.....	32
6.8	STORAGE SECURITY.....	32
6.9	CARGO TRACKING AND INTEGRITY.....	32
6.10	GLOBAL HARMONIZATION.....	32
<b>7</b>	<b>SECURE AIRSPACE.....</b>	<b>34</b>
7.1	INTEGRATED RISK MANAGEMENT .....	34
7.2	VERIFIED AIRSPACE ACCESS .....	34
7.3	SECURITY RESTRICTED AIRSPACES.....	35
7.4	AIRSPACE VIOLATION DETECTION, ALERTING, AND MONITORING.....	36
7.5	INTEGRATED MANAGEMENT OF AIRSPACE SECURITY.....	37
7.5.1	Noncooperative Surveillance .....	37
7.5.2	Countermeasures.....	37
7.5.3	Joint Exercises .....	38
7.6	COUNTER PROJECTILES.....	38
7.6.1	Airport AOA/Terminal Airspace .....	38
7.6.2	Aircraft/Flight Object.....	39
<b>8</b>	<b>SECURE AIRCRAFT .....</b>	<b>40</b>
8.1	INTEGRATED RISK MANAGEMENT .....	40
8.2	AUTHORIZED CONTROL OF THE AIRCRAFT .....	40
8.2.1	Cockpit Systems.....	40
8.2.2	Onboard Personnel.....	40
8.3	AIRCRAFT MONITORING/SURVEILLANCE.....	41

8.3.1	Cockpit, Cabin, and Cargo Hold Surveillance.....	41
8.3.2	Continuous Air Monitoring.....	41
8.4	AIRCRAFT HARDENING AND DEFENSIVE SYSTEMS .....	42
8.5	SAFETY INTEGRATION.....	42

## LIST OF TABLES

Table C-1.	Significant Security Transformations .....	3
------------	--	---





## LAYERED, ADAPTIVE SECURITY SERVICES (ENTERPRISE OPERATIONS)

### 1 INTRODUCTION

#### 1.1 OVERVIEW

This concept of operations (ConOps) for the Next Generation Air Transportation System (NextGen)<sup>1</sup> has incorporated an effective security system without unduly limiting mobility or making arbitrary intrusions on the civil liberties of all users by embedding layered, adaptive security measures throughout the air transportation system, from reservation to destination. This NextGen Security concept addresses the following: 1) Integrated Risk Management, 2) Secure People, 3) Secure Airports, 4) Secure Checked Baggage, 5) Secure Cargo/Mail, 6) Secure Airspace, and 7) Secure Aircraft.

The security system has particularly strong interrelations with NextGen Shared Situational Awareness, airports, and global harmonization capabilities along with some aspects of Agile ATM. Cyber security is addressed in the Net-Centric Infrastructure (NEI) Services, Chapter 4, and Shared Situational Awareness (SSA) Services, Chapter 5. Non-cooperative surveillance is addressed in Chapter 5.

Layered, adaptive security is defined as a risk-informed security system that depends on multiple technologies, policies, or procedures adaptively scaled and arranged to defeat a given threat. This adaptability further permits the use of increased variability in system operations that creates additional uncertainty for the terrorist. Adversaries cannot defeat one particular security measure and system and thereby achieve a “break-through,” which permits them to operate freely with no further barriers to their activities. Furthermore, the security system has the adaptability to scale its systems and procedures to the risk level of a threat in a given situation rather than being bound to an inflexible “one size fits all” approach.

Given the limited resources of government and private industry, it is critical that mitigation measures be developed based on threat and vulnerability, as well as the potential consequences to individuals, transportation assets, and the economy.

The NextGen approach better matches system costs with the risk assessment and the capacity demands at various airport and screening locations.

To achieve the requisite adaptability while maintaining effective security standards, the NextGen security system must have a sound method of prioritizing risks and assessing the proportional effectiveness of different ways of countering them. The Secure-Integrated Risk Management process performs this essential function that then directs the deployment of equipment, personnel, and procedures and policies to defeat the evolving threat. The remaining capabilities

<sup>1</sup> The term “NextGen” in this document applies solely to the JPDO Enterprise Architecture and ConOps for 2025. No other program is referenced or intended by this term.

described at a high level in this chapter must be the consequence of integrated risk management (IRM) assessments.

## 1.2 NEXTGEN SECURITY MANAGEMENT AND COLLABORATIVE FRAMEWORK

In the NextGen, the security system is better integrated with other National Airspace System (NAS) functions, and through advanced networking functionality, linked to external aviation industry stakeholders and non-Federal government entities. To maintain effective security management across major stakeholders, a collaborative framework is composed of the following key functions and processes identified below.

**National Aviation Security Policy.** NextGen security policy embraces a broad view of threats, including direct attack, exploitation, and transfer; recognizes interdependencies and uncertainty; nurtures virtual or extended enterprises supported by connectivity of diverse, informed stakeholder partnerships; employs layered security using physical, process, and institutional layers; accounts for systemic vulnerabilities that are created by the networked nature of the aviation system; and creates resilience in the system to mitigate potential incident consequence. The NextGen has achieved integration with the overarching Homeland Security Presidential Directives and their subsidiary documents.

- **Aviation Security Stakeholder Involvement.** NextGen Stakeholder Involvement fosters industry, federal, and local partnerships with clearly defined roles and responsibilities for prevention, protection, response and mitigation, and recovery operations at strategic, operational, and tactical levels. Collaborative decision-making contributes to a positive security culture. Rapid decision-making based on shared situational awareness is achieved through advanced communication and information sharing systems.
- **Integrated Risk Management.** NextGen IRM includes prognostic tools, models, and simulations at the strategic, operational, and tactical level to support all stakeholder decisionmakers and managers in the grafting of cost-effective “best practices” into the design, acquisition, deployment, and operation of aviation security system assets and infrastructures. Knowledge bases concerning threats, vulnerabilities, and practices are tailored to user profiles that proactively determine need/authorization to know.
- **Aviation Security Implementation.** NextGen Implementation capabilities encompass a robust set of strategic, tactical, and operational capabilities and services focused on prevention, protection, response and mitigation, and recovery initiatives that are undertaken by various stakeholder organizations.
- **Aviation Security Assurance.** NextGen Assurance capabilities include various certification programs administered by federal, industry, and local stakeholders, surveillance and evaluation activities administered and performed by various stakeholders, enforcement inspections performed by federal stakeholders and local stakeholders, and incident investigations performed and administered by various stakeholders.

## 1.3 NEXTGEN SECURITY OPERATIONAL IMPROVEMENTS SUMMARY

Table C-1 lists the major operational improvements that the NextGen Security system provides compared with the NAS of 2006.

**Table C-1. Significant Security Transformations**

Significant Transformation	2006 Current Capability	2025 NextGen Capability
Integrated Risk Management	<ul style="list-style-type: none"> <li>Static facility or passenger risk assessments</li> </ul>	<ul style="list-style-type: none"> <li>Dynamic risk assessment management process produces real-time risk profiles for aviation facilities and flight object.</li> </ul>
Checkpoint Operations Responsibilities	<ul style="list-style-type: none"> <li>US Government (USG)/TSA responsible for policy development and execution</li> </ul>	<ul style="list-style-type: none"> <li>Government, airport operator, or third-party decentralized while observing common standards developed by USG</li> </ul>
Credentialing/Authentication	<ul style="list-style-type: none"> <li>Badges, background checks (mainly manual based)</li> </ul>	<ul style="list-style-type: none"> <li>Biometric credentials with 1-second authentication at access or screening checkpoints</li> </ul>
Baggage Screening Technology	<ul style="list-style-type: none"> <li>Large footprint baggage screening devices—most not integrated with baggage system—only detect explosives. Separate boxes for chemical, biological, radiological, nuclear, and explosives (CBRNE) sensors</li> </ul>	<ul style="list-style-type: none"> <li>CBRNE detection systems incorporating sensor fusion, with a range of sizes and throughput capacity from high throughput in-line systems to smaller units for remote screening, local airports. Some are small, lightweight, and portable devices that can screen bags from standoff distances.</li> </ul>
Passenger Screening	<ul style="list-style-type: none"> <li>Metal detector-based, relatively large explosive trace detection (ETD) air sampling equipment/portals</li> </ul>	<ul style="list-style-type: none"> <li>Sensor arrays deployable throughout terminal enabling rapid movement of passengers through virtually invisible screening points—fast and efficient—centralized monitoring center reduces security footprint at checkpoint. Advanced behavior profile recognition (BPR) procedures. Biological threat and disease detection and assessment.</li> </ul>
Chemical, Biological, Radiological, Nuclear, Explosives (CBRNE) Detection	<ul style="list-style-type: none"> <li>Only deployed at a few high-threat locations (typically not airports)</li> </ul>	<ul style="list-style-type: none"> <li>Deployable for all airport screening operations, link by network-enabled infrastructure (NEI) to airport operations, law enforcement and national network</li> </ul>
Security System Deployability	<ul style="list-style-type: none"> <li>Expensive slow installation</li> </ul>	<ul style="list-style-type: none"> <li>Rapid deployable units for low-capacity, temporary and intermittent screening locations integrated with other airport customer service functions</li> </ul>

**Table C-2. Significant Security Transformations (continued)**

Significant Transformation	2006 Current Capability	2025 NextGen Capability
Screening Checkpoint Location	<ul style="list-style-type: none"> <li>In airport terminals between public area and “sterile” area</li> </ul>	<ul style="list-style-type: none"> <li>Remote Terminal Security Screening (RTSS) enabling all or portion of security screening to be conducted off-airport.</li> </ul>
Man Portable Air Defense System (MANPADS) (e.g., shoulder-fired missiles, lasers, electromagnetic pulse [EMP]) Detection and Defeat	<ul style="list-style-type: none"> <li>Perimeter and adjacent jurisdiction observation by law enforcement officers (LEO)</li> </ul>	<ul style="list-style-type: none"> <li>Onboard aircraft leveraged safety modifications, supplemented by ground-based and procedural systems</li> </ul>
Commercial Spaceport	<ul style="list-style-type: none"> <li>Licensing with no commercial passenger service</li> </ul>	<ul style="list-style-type: none"> <li>Passenger screening and bilateral agreements for international reentry of hypersonic vehicles</li> </ul>
Security Relevant Information	<ul style="list-style-type: none"> <li>Disparate, stand-alone systems; no easy transfer of data.</li> </ul>	<ul style="list-style-type: none"> <li>Network-centric information access with “smart” applications proficient in data-mining and pre-analysis of large amounts of data. Decision support applications assist the security operations center and other security analysts.</li> </ul>
Cargo Screening Technology	<ul style="list-style-type: none"> <li>Small percentage of cargo being screened for explosive threats</li> <li>Most cargo undergoes paper-based documentation (known shipper)</li> </ul>	<ul style="list-style-type: none"> <li>All air cargo items not packed in sterile area and securely conveyed to aircraft are screened for CBRNE.</li> </ul>

## 2 INTEGRATED RISK MANAGEMENT

Risk management is the ongoing process of understanding the threats, consequences, and vulnerabilities that can be exploited by an adversary to determine which actions can provide the greatest total risk reduction for the least impact on limited resources. Risk management is continuous; it is conducted from the strategic to the tactical levels. In this section, the strategic aspects of the IRM process are described. The following sections briefly mention the relevant tactical aspects of IRM for that particular threat vector. The NextGen layered, adaptive security's IRM capability is an overall federated risk assessment and risk mitigation framework for guiding multiple security service enterprises to assist in making decisions, allocating resources, and taking actions under conditions of uncertainty. This framework is a planning methodology that outlines the process for setting security goals through a) prevention, b) protection, c) response and mitigation, and d) recovery. It derives its importance from the following needs:

- Understand the spectrum of threats that could be mounted against the NextGen.
- Identify the vulnerabilities that can be exploited by an adversary.
- Evaluate and prioritize assets and activities to be protected from attack.
- Determine which protective actions can provide the greatest total risk reduction for the least impact on limited resources.
- Provide the most focused and adaptive security measures to reduce the impact of security systems and procedures on air transportation.

IRM is characterized by a specific and consistent terminology to describe its various aspects. Threats are the likelihood of a terrorist attack on a particular asset. Vulnerabilities are weaknesses in the design, implementation, or operation of an asset or system that can be exploited by an adversary or disrupted by a natural disaster. Consequences are the result of an attack on infrastructure assets reflecting level, duration and nature. Risks are measures of potential harm that encompasses threat, vulnerability, and consequence.

The assessment of risks provides a prioritized list of vulnerabilities and potential mitigation strategies. The terrorist has freedom to choose targets and modes of attack; therefore, the NextGen Security system must develop (but not necessarily universally deploy) operationally feasible mitigations to as many potential threats as possible. Because of limited resources, mitigation requiring substantial investment (e.g., system cost or infrastructure intensive) is applied (deployed) in the order of risk level. For example, external attacks on aircraft may be an issue at some airports requiring mitigation. This does not mean that General Aviation airports will have or need such systems.

Another way to stretch resources is through technical advances in sensor design and fusion and in cost efficiencies typical of information processing system upgrades. With the development of low-cost CBRNE sensors for low-volume operations, it is possible to conduct screening in 2025 at sites that would have been economically infeasible in 2006 for a given risk profile (thus permitting many more airports to provide commercial service). This does not mean that all noncommercial operations need to screen passengers or cargo for flights posing below threshold risk levels. Many flight operations occur far from major metropolitan areas or national security restricted areas. However, flight operations to sensitive areas need to make adjustments to reduce their risk profile.

In summary, it is essential to remember that the security system responses and procedures throughout the NextGen are applied based on the risk profile of each flight object and airport facility. Facilities or flights that do not adopt particular security processes may still operate in the *NextGen* but may need to observe some restrictions depending on the given risk profile created. Yet, their overall access and performance in *NextGen*, even with some (self-imposed) security restrictions, is considerably greater than their access in 2006.

## 2.1 RISK MANAGEMENT PROCESS

The primary objectives of the risk management process are evaluating the effects of defined threats, assessing the vulnerability, and evaluating and prioritizing assets and functions for a civil aviation system that is a significant target for our adversaries, including high-value localized targets. The IRM process divides risk management into phases:

- Threat analysis
- Vulnerability analysis and consequence assessment
- Countermeasures definition
- Countermeasures prioritization and acquisition strategy analysis
- Procedural and technology insertion with subsequent evaluation.

With the continuous review of threat vectors, objects, and materials, coupled with intelligence on current national threat levels, civil aviation passengers assure that security stakeholders are prepared with timely and appropriate threat information. IRM provides capabilities for stakeholders to collaborate and to facilitate integrated decision-making. Collaboration may occur for strategic or tactical intent. The countermeasures analysis and prioritization include a comprehensive mix of policies, procedures, technologies, and communications between stakeholders appropriate to the alternatives enumerated.

The monitoring and analysis process is inherent in the five phases of risk management to not only evaluate the effectiveness but also refine IRM decisions continuously.

## 2.2 SECURITY RISK MANAGEMENT

The five phases of risk management mentioned above are applicable to the full spectrum of timeframes, ranging from strategic (years/months/days) to tactical (days/hours/real-time). Each phase must be integrated into each NextGen security layer. In this section, the strategic aspect related to each security layer is included. For the tactical aspect of each security layer that specifies how the IRM strategies are employed in a given domain, refer to the specific security layer IRM sections. The NextGen IRM capability enables the development of risk-based assessment strategies, vulnerability analyses, and complete compendiums of attack consequences related to threats for the NextGen. This capability also ensures the operational validity of the *risk profile of the flight object* and the *risk profile of the aviation facility*. These two profiles play a crucial role in governing how the NextGen Security system will implement its operational procedures in specific circumstances.

### 2.2.1 IRM—Secure People

The IRM—Secure People capability enables the development of risk-based assessment strategies, analyses of vulnerability, and estimation of attack consequences related to screening people at check-points, passengers, and aviation workers for the NextGen. One major function within the IRM—Secure People is to define the watch lists and factors that determine the relative risk ratings. Those airport workers with continued access would be required to undergo periodic (random) and regularly scheduled updates of their security and risk profile. Passengers and aviation workers are checked against these lists to assess their risk level. In addition, IRM—Secure People capability also identifies behaviors associated with high-risk people that airport security personnel could use in surveillance.

Key to the selection of appropriate risk management strategy is the comprehensive analysis of threat event mitigation procedures. Often, this is accomplished through operational threat scenario analysis. For instance, countermeasures for a checkpoint breach scenario include an analysis of the range of effects and mitigation strategy for the mitigation of those effects. Although technology insertion is a vital part of the IRM—Secure People countermeasure strategy, it is important to regard the technology (or combination of technologies) as only one piece in the decision chain. Of equal importance to the technology selected is the promulgation of appropriate policies for the use of technology (e.g., carry-on baggage alarm resolution processes) and appropriate search strategies to be applied. Coupling various capabilities (e.g., watch lists and behavior profiles) can maximize the threat detection capabilities of each, if carefully integrated.

### 2.2.2 IRM—Secure Airports

Security of NextGen Airports is central to preventing attacks against aircraft within the airport terminal area, either from local intrusion or attacks carried out on the ground, by intrusion onto the airport operations area (AoA), the public area, the sterile area, the remote facilities, or from the air. In addition to routine screening of passengers, bags, and cargo, airports also screen for threat all concessionaire materials for resale, goods, and liquids. Attack targets vary greatly: people, fuel farms, tower, operations centers, electrical infrastructure, and aircraft. Projectile or Man Portable Air Defense System (MANPADS) attacks from beyond the perimeter of the airport are also included in the individual airport's threat profile.

The NextGen IRM—Secure Airports capability enables the determination of the risk profile of the aviation facility and the identification of the high-risk airports and related facilities that require additional security resources, technology investments, and more robust security operations to receive the appropriate levels of protection. The process also identifies airports that have low-risk profiles that do not mandate much if any security upgrade. Many criteria are used to determine risks, for example—

- High-demand airports with large enplanements and international operations
- Airports in designated high-risk geographic locations
- Airports with special events/activities (e.g., frequent VIP presence).

Each airport above a defined risk profile threshold performs a threat and vulnerability analysis that is updated periodically. The vulnerability analysis includes the entire physical footprint of the airport, out to the fence line and beyond to include the MANPADS threat. Each airport must develop and implement an airport security protection plan based on sound practice and pertinent airport security design.

Assessments and priorities as to probabilities of attack follow from the five steps enumerated in Section 2.1. Such analyses indicate the most appropriate direction for the application of countermeasure and mitigation procedures and resources in the airports, including airport terminal building public area, at the screening checkpoints, inside the concourse sterile areas,<sup>2</sup> and on-the-air operations area. Passenger prescreening, passenger boarding physical screening, and carry-on baggage screening system capabilities respond to the risk profile and threat situation provided by IRM (e.g., higher alert state, special events, high risk airports) with various measures.

Selected prioritization strategies to enhance the robustness of Airport security include an appropriate mix of people, procedures, infrastructure, and technology specific to the alternatives analyses and the countermeasures analyses. Similar to IRM—Secure People, technology investment is only one piece in the overall risk management of airports and is balanced with policy and procedures.

### 2.2.3 IRM—Secure Checked Baggage

The NextGen IRM—Secure Checked Baggage capability performs assessments and develops priorities as to probabilities of attack with various threat objects. Threat objects for checked baggage include explosives and improvised explosive devices (IED), CBRN materials, and other hazardous materials. Such analyses provide the most appropriate strategy for the application of countermeasure and mitigation procedures and resources. For example, as the Secure People capability identifies higher risk passengers, they should receive more stringent screening; however, there is a concomitant cost of resources and screening time depending on the criterion values for different levels of risk. The IRM Secure Checked Baggage process analyzes the various costs and benefits with the mitigation procedures to arrive at the best balance of threat reduction for the available resources and other constraints.

Similar to the discussions in previous sections, using detection technology as a risk mitigation strategy is incomplete without considering policy, procedures, and other strategies. Technologies are useful only to the degree that they assist the human operator in decision-making. In addition, the “throughput” of the technology has a major impact on the processing rate of baggage and thus has impact on overall aviation commerce and system efficiency.

### 2.2.4 IRM—Secure Cargo/Mail

The NextGen IRM—The Secure Cargo/Mail capability process assesses risks for cargo/mail throughout the shipping chain from source to exit from the NextGen. The shipping chain includes cargo source, containerization, freight consolidation/forwarding, cargo/mail screening

---

<sup>2</sup> Secured areas are those that require positive identification with credentials (badge, smart card, etc) and controlled access.

locations, air transport to destination, and all intermediate storage and transport. (The Cargo Source is defined as the entity in physical possession of the cargo immediately before transfer into an approved sterile area for assembly and packing or approved cargo screening system operation.)

The risk assessment is based on the freight management system information supplied by the NextGen Secure Cargo/Mail capability. IRM—Secure Cargo/Mail can identify the risk level of given types of cargo (e.g., difficulty in screening) and the risk profile of the flight object and the aviation facility. Such analyses use many criteria to determine risks, for example:

- Volume and types of cargo (e.g., break bulk, containers, commodities)
- Operators (e.g., airlines, airports, shippers) cargo integrity procedures
- Cargo geographic origin(s) and routes
- Passenger flight or cargo flight
- Size/weight of aircraft
- Cargo operations' proximity to the traveling public at the airport.

Threat objects for cargo and mail include explosives, CBRN materials, and other unapproved hazardous materials. The risk profiles determine appropriate detection capabilities and procedures for mitigating the risks of penetration and attack through cargo/mail. For example, screening for “live cargo” must be processed very differently from other cargo.

For higher risk operators and operations, IRM—Secure Cargo/Mail develops strategies for specific mitigation measures. Depending on the risk type and level, such measures may include additional screening by shipper, airport, air carrier, or security service provider (SSP); detection technology deployment; extra placement of cargo security screeners; use of canine detection teams; and more frequent inspections of cargo operators and procedures for diverting some (slightly) higher risk cargo from passenger flights to ground transport. In addition, IRM—Secure Cargo/Mail coordinates with the Secure Airports (see Section 4) capability to develop appropriate airport requirements to mitigate cargo operations risks at airports (e.g., where to place cargo operations at a high-enplanement airport). IRM—Secure Cargo/Mail has integration requirements with the “Secure Aircraft” capability to develop appropriate measures for cargo protection on board the aircraft—container and cargo hold.

### **2.2.5 IRM—Secure Airspace**

The NextGen IRM—Secure Airspace capability identifies locations of national critical infrastructure, assets, population centers, and activities (e.g., national sports events) that might warrant additional airspace protection. Using the locations identified, the IRM—Secure Airspace determines an airspace risk profile based on the IRM risk assessment process. These risk profiles guide flight planning, security restrictions, and response to anomalies/incidents. The risk assessment criteria include many variables like size and performance of aircraft, type of operator (e.g., general aviation, commercial passenger airline operations) domestic or international traffic and proximity or actual access to the airspace.

The IRM—Secure Airspace process drives the development of risk-based access criteria that the Secure Airspace (Section 7) capability uses to set the integrated aircraft's security profile—for

example, people and baggage prescreened (Secure People and Secure Checked Baggage capabilities), cargo prescreened (Secure Cargo capability), weight class of aircraft, and acceptable security factor (see Secure Aircraft, Section 8; Total Flight Monitoring concept described in Chapter 2). The IRM—Secure Airspace determines the risk likelihood of various types of operations. IRM also develops airspace access strategy for Secure Airspace (Section 7) to implement. For example, IRM can determine a certain weight class of aircraft poses lower risk (e.g., low end of general aviation [GA] aircraft or that unmanned aircraft system [UAS] operations above a certain weight size requires special restrictions).

### 2.2.6 IRM—Secure Aircraft

The NextGen IRM—Secure Aircraft capability assesses the likelihood of risks for various aircraft types. This would include risks to the aircraft itself, as well as the risk of the aircraft to be used as a terrorist instrument. Criteria used for determining the risk factor for aircraft include the following:

- Aircraft size and weight
- Amount of fuel on board
- Passenger and or cargo flight
- Number of passengers
- Origin/destination/path/time of flight
- Flight screening results—whether there are higher risk passengers or cargo on board
- Presence of law enforcement officers (LEO) on board.

Based on the risk assessment results, IRM—Secure Aircraft develops risk mitigation strategies that can deliver varied levels of security performances for the aircraft:

- Install sensors on board, such as—
  - CBRNE sensors in cargo hold
  - Video monitoring in passenger cabin
  - Continuous air monitoring
- Harden aircraft frame or other structures
- Deploy security personnel on board
- Install MANPADS countermeasure technology or implement countermeasure procedures
- Implement biometrics control for cockpit access
- Implement special security procedures
- Require high availability air-to-air and air-to-ground communication.

The IRM—Secure Aircraft capability also develops risk envelopes for the NextGen security factor to be used by the total flight monitoring capability. This value is not meant to be simply a singular value; it could be a “profile” that depicts the “risk” aspect of a particular flight.

Similar to discussions given in previous sections, it is important to balance the selection and use of technology (or combination of technologies) with policies, procedures, and economics impact. To the extent possible, safety-based aircraft modifications are leveraged for mitigation of security risks.

## 2.3 NEI-ENABLED INTEGRATED RISK MANAGEMENT COLLABORATION ENVIRONMENT

As discussed in previous sections, Security IRM uses the NextGen NEI capability to receive all applicable, authorized information within the NextGen as inputs to IRM's risk assessment analysis and then to distribute outputs from the IRM process to all the authorized stakeholders as needed. In addition, the SSP-based IRM provides various analytical capabilities and information sharing environment to collaborate with the stakeholders, either in strategic timeframe (months/days/hours) or tactical timeframe (hours/minutes/real-time). Built on a NextGen NEI foundation, NextGen IRM makes use of a federated risk assessment collaboration infrastructure, which is provided by security stakeholders to perform, for example—

- Collaboration and communication capabilities
- Aviation system monitoring
- Risk analysis tools
- Risk scenario modeling capability suitable for the stakeholder mission
- “What-if” and decision support capabilities to assess efficiency and effectiveness of risk mitigation strategies to support strategy development such as
  - Investment portfolio (e.g., combination of technology deployment/personnel/infrastructure to high risk airports)
  - Technology insertion
  - Adaptive security measures for security layers
  - Resource and asset reallocation (e.g., allocation of baggage and cargo screeners and deployment of MANPADS countermeasures at airports)
  - Technology tailoring (e.g., sensitivity and throughput of sensors)
  - Procedure changes (e.g., screening and alarm resolution)
  - Airspace restrictions
  - Traffic flow changes
- Security alert identification, reporting, and status determination and escalation.

Because the NextGen security risk management stakeholder community is diverse and involves multiple government organizations that interact with their constituents and users, the NextGen IRM has a unified command, control, and communication (C3) framework for integrated risk management decision-making.

This unified C3 has the following foundational aspects:

- Clarity of roles and responsibilities of NextGen security stakeholder group for various aspects of IRM. The stakeholder group includes the SSP, defense service provider (DSP), air navigation service provider (ANSP), aviation system users, aviation transport, and airport authorities
- An established set of standard operating procedures (SOP) that change to meet evolving threat
- Well planned logistics for preparedness, response, and recovery
- Robust training and joint exercises.

This operational framework for the unified C3 enables the NextGen IRM stakeholder group to coordinate its decisions and actions in a timely manner across all aspects of performance. NextGen capabilities based on operational improvements in technology and procedures are seamlessly integrated with security processes to meet the needs of multiple areas (e.g., flight object security, ATM, airport facility security).

## **2.4 RISK MANAGEMENT STRATEGY MONITORING AND FOLLOW-UP**

To assess how well the risk management process works and continue to refine NextGen risk strategies (mitigation and execution), the IRM process uses operational data to constantly update and refine its methods and outputs.

NextGen IRM has a monitoring and follow-up capability that includes the following:

- Data collection and analysis
- Metrics analysis
- Risk management modification process—for example,
  - Changes of criteria and input parameters used in all the steps of the risk management process
  - Changes in risk scenarios (modified and/or new ones)
  - Changes in security envelop threshold (e.g., for the security factor in the total flight monitoring capability).
- Identification of gaps and areas for improvements in, for example—
  - Technology
  - Infrastructure
  - Process and procedures
  - C3 roles and responsibilities
  - New stakeholders.
- Tracking of follow-up actions.

Inherent in the process would be the supervision and analysis process for the five phases of the risk management process. A set of testing and evaluation procedures is institutionalized in sequence to evaluate the effectiveness of all five phases.

### 3 SECURE PEOPLE

No aspect of the NextGen security architecture is more important to the perception of a secure aviation system environment than publicly visible or implicit checkpoint and carry-on baggage screening operations. Other less visible security procedures may work similar ends and do so as effectively. However, the visible aspect of checkpoints and baggage screening is still most tangible and hence most relied on by the public in establishing its level of confidence and thereby its use of the system. The checkpoint displays an operating profile of consistency and routine, while behind the scenes, it has several new screening techniques and tools that can be leveraged for the assessed risk, and occasionally, performed randomly as an added measure.

In the NextGen, the Secure People capability of the security architecture puts greater reliance on a more integrated approach correlating credentialing and identification processes with screening. Aviation security risks are mitigated by identifying and preventing people who, whether travelers or aviation workers, are a potential threat from gaining access to the air transport system through prescreening and credentialing, screening, and intervention. For travelers, aviation security is provided continuously from the time the reservation is made until the safe arrival of the flight at the final destination airport. For aviation workers, a standardized credentialing process and identification technologies prevent unauthorized individuals to access restricted areas of the airports. Those airport workers with continued access would be required to undergo periodic (random) and regularly scheduled updates of their security and risk profile. The NextGen Net Enabled Operations ([NEO]; the decision support and other applications using NEI for information transfer and retrieval) permits more valid and faster credential verification. A balance between security and customer service is maintained, permitting the consistent, efficient, and seamless movement of passengers at the airport.

#### 3.1 INTEGRATED RISK MANAGEMENT

Continuous threat assessment and risk management processes identifies vulnerabilities and risks associated with people, whether travelers or aviation workers, moving within aviation facilities and the air transportation system. Mitigation strategies and countermeasures depend on threat/alert levels. Integrated decision increases decision quality and decrease response time to events. (See Section 2, Secure People.)

#### 3.2 AUTHENTICATION AND CREDENTIALING

Authentication and credentialing processes are performed for passengers and the full range of aviation system employees, including airport, airline, vendors, maintenance and utilities, law enforcement, and government service providers (ANSP, SSP, DSP). Credentialing in this context is essentially the granting of a right of access while authentication is the verification of that right of access in a given situation or time. The positive identification of people is part of the layered, adaptive security system, which are based on levels of security, location, and net-centric information sharing. NEI operational linkages directly connect distributed users, enabling a more transparent and less interactive process and reduced transaction times. Biometric identity management ensures that passenger identities are preserved despite name and/or address changes, and mitigate the use of fraudulent credentials. All persons entering any virtual or physical secured area of the civil aviation system are automatically assessed and verified and,

where appropriate, their identities are verified by NEI-linked biometrics. Biometric identification validation and authorization verification for this purpose is a key component to the screening system.

### 3.2.1 Credentialing

NextGen Aviation credentialing programs conduct background checks of aviation industry employees based on biographic and biometric information. Aviation workers include airport and airline employees, vendors, shippers, and service providers for the operations and maintenance and the service of aircraft, cargo, aviation facilities, and aviation infrastructure. The person's identity is authenticated on attributes permitting positive identification for access to secured areas (e.g., tarmac, aircraft, and cargo and baggage conveyances).

Passenger credentialing programs permit passengers certain access rights or privileges that are unavailable to noncredentialed passengers. The credentialing process is conceptually similar to that performed with aviation system employees; although obviously the kinds of information needed to receive the credential vary.

### 3.2.2 Passenger Authentication

Prescreening is the process of checking passenger information against government watch list information or noting the absence of expected confirmatory data to the query to determine the risk status of that individual to enter the concourse sterile area<sup>3</sup> of the airport and/or to board a commercial flight. The relatively lengthy period of time between reserving a flight and the actual departure date for the majority of passengers provides an opportunity to assess risk before individuals even arrive at the airport. However, the NEO capability allows 1-second verification so that on-demand passengers using an air taxi or very light jet (VLJ), with appropriate credentials, can be effectively verified before flight. Prescreening of individuals occurs every time a flight reservation is made. A flight reservation may include the itinerary of one or more individuals. All individuals on the reservation are prescreened before their arrival to the airport.

The NextGen passenger prescreening leverages advances in information technology (IT) systems provide data sources and seamless information flow from passengers as they travel through the airport. Prescreening compares reservation information against known and validated threat and vulnerability information before local and/or remote check-in. Depending on prescreening results, a small percentage of individuals are required to further verify their identity. Even before a passenger checks-in at the airport or remote site, uplinked information could be made from his/her handheld devices to register identification information (e.g., biometrics, digital photo, or biographical data) to verify that the passenger is not a match to a government watch list or that verification information meets criteria.

As part of the prescreening process, most individuals are able to travel expeditiously through the checkpoint and into the sterile areas. Those persons exceeding certain risk levels (without being identified as no-fly) receive enhanced screening at passenger security checkpoints in addition to more intensive checked baggage screening of any checked bags. The NextGen prescreening process includes a degree of randomness in occasional selection of individuals for secondary

---

<sup>3</sup> A sterile area is one in which passengers have been through security checks.

screening. Some airports may opt to allow passengers and nonpassengers through the security checkpoint. In this scenario, nonpassengers must have adequate credentialing.

Consistent with civil liberties, identity verifications are performed locally or through net-enabled operations at each transaction such as when reservations are placed, before check-in, or when a person seeks to pass through an airport's access control point, to enter a sterile area or to board an aircraft. Privacy is maintained by advanced encryption and assembly of segmented data as a virtual temporary data object for authentication. Upon completion of the transaction, the data segmentation is restored with only a record log that an authentication event occurred. Derivative threat assessment values enable the activation of adaptive screening or other security systems, protocols or procedures. Some measures must apply to all threat levels, guarding against terrorist or criminal threats to the aviation system.

### **3.2.3 Aviation Industry Worker Authentication**

The authentication programs also exist for aviation system employees (e.g., airport workers, airline employees, vendors, and LEOs) when they access various parts of the NextGen in performing their duties. The person's identity is authenticated on attributes permitting positive identification for access to sterile and or secured areas (i.e., those areas with access controls). Net-enabled operations linkage enables a more transparent and less interactive process and thus reducing transaction times, enabling 1-second identification on demand. All persons entering any virtual or physical aspect of the civil aviation system requiring credentials is automatically assessed, and where appropriate, their identities are verified by NextGen biometric information. This action applies at many locations, but notably at access points to secured areas of airports and at the checkpoints where persons (e.g., armed law enforcement officers) seek to pass into the sterile area. Biometric identification validation and authorization verification for this purpose is a key component to the screening system. On the positive side, the primary benefit of integrating the prescreening function with credentialing systems is to reduce the number of unknown travelers and to improve accuracy of prescreening results. The transportability of aviation worker credentials to other airports also is facilitated.

Access controls and biometric verification systems are used to prevent unauthorized individuals from entering secured areas. Depending on enhanced security requirements of more tightly controlled areas (e.g., fuel farms, navigation systems, cockpit, tower, command center), individuals require multifactor authentication (i.e., use of multiple access control methods). One potential access control scheme for a particular class of workers is a combination of one or more biometrics, a password, and radio frequency (RFID) card. For example, a maintenance worker who needs access to sensitive surveillance equipment must authenticate with a biometric, time-sensitive, and variable personal identification number (PIN). However, even before arriving at the secure area, the worker would need to use his identification card, which includes RFID technology for uploading the timestamp and access point onto the secured area.

## **3.3 CHECKPOINT PERSON SCREENING**

The NextGen Secure People capability also includes checkpoint screening of persons and carry-on baggage. Checkpoint person screening primarily involves travelers with flight reservations, but may include other credentialed or noncredentialed airport, airline personnel, crew member,

or private individuals authorized to enter the sterile area of an airport. Through the NEO capability, passenger screening includes data from risk assessment, behavior analysis, and global exchange of traveler information.

Passenger screening systems detect CBRNE and weapons, are relatively unobtrusive, and have lower “hassle factor.” The aviation people security screening system must be just visible enough to provide a level of deterrence, giving perpetrators pronounced uncertainty for a successful outcome of a planned malicious event. The addition of a small, random selection of individuals for enhanced (secondary) screening is evident for this reason.

Screening consists of a combination of sensors for CBRNE and weapons detection. The biological sensors can also sense certain symptoms of active disease such as elevations of body temperature. The NextGen person screening systems have small footprints as a result of sensor fusion and can be easily scaled for different size airports’ physical space and throughput requirements. Because of the accuracy of these systems, passengers rarely experience unplanned additional screening or inquiries from security personnel. If a threat object is discovered, the screening equipment alerts NextGen NEO applications, which immediately correlate other current data concerning the individual (e.g., carry-on and checked bags in the system, flight reservation data, and credential and prescreening data) to determine whether other potential threats might remain in the system.

### **3.4 CHECK POINT BAGGAGE SCREENING**

To permit maximum passenger convenience, the NextGen security system generally allows passengers some carry-on baggage, the main exception being in the highest condition of alert. Checkpoint baggage screening functions are as follows:

- Carry-on baggage screening
- Situation response procedures
- Alarm resolution procedures
- Threat object control procedures.

In the NextGen, the checkpoint screening systems are system engineered with various sensors combined into “one box” by advances in sensor fusion. These detection units have modular components and easily replaceable “firmware”; therefore, they are able to be easily modified to detect the changing range of threats and servicing while simultaneously minimizing the checkpoint “footprint” and configuration requirements. Thus, they can be placed in various locations in the airport with minimal “fit” problems needing to be resolved. For high-capacity airports, appropriately equipped nearby areas are provided for the purposes of the discreet alarm resolution of passengers and/or their carry-on baggage. Checkpoint screening is as automated as possible in an effort to increase throughput and minimize the number of screeners needed. The checkpoint control procedures and access control technologies preclude people from entering the sterile area through the passenger exit lane bypassing the checkpoint screening function.

The checkpoint has a central command center function linked to the airport Security Control Center (SCC) through NEO to handle the two-way information flow with the checkpoint, the airport, and other SSP operational centers. If a threat object is identified, the screening

equipment, through NEI, immediately triggers the NEO security system to correlate other current data on the individual (e.g., person screening systems, checked baggage in the system, flight reservation data, and credential and prescreen data) to determine whether other threats might remain in the system.

Checkpoint screening systems undergo certification approval in accordance with NextGen standards for checkpoint CBRNE and weapons detectors. The SSP approves checkpoints as complete units. The checkpoint concept includes detection capability for the amounts, types, and configurations of explosive threat types, weapons and chemical and biological agents through the use of chemical identification detection devices, and nuclear and radiological threat types. Sensors are oriented to permit the passenger to proceed through a short passageway, making his/her way through a series of sensors. An alarm shunts the passenger off to an alarm resolution area in the checkpoint. The passenger's carry-on baggage proceeds down a separate passage proceeding through a series of detection devices to detect the presence of carry-on baggage threat types. If an alarm occurs on the passenger or his carry-on baggage, both are reunited for a second level of screening procedures and interaction with the passenger to resolve the alarm. If the alarm cannot be resolved, additional procedures are employed, up to involving the use of LEOs.

Through the NextGen Airport design process, physical space is allocated to the discrete resolution of bags and/or passengers that trigger alarms well outside the flow of cleared passengers and bags. The increased accuracy of detection sensors minimizes the frequency of this secondary screening response. In addition, the increased specificity of the alarm permits more focused resolution procedures and faster go/no-go decisions. If a threat object is identified, control procedures and technologies are readily available for using qualified law enforcement people to safely contain the object. Redundant NEI communications links to the airport security coordinator, law enforcement, air carriers, and airport SCC are provided.

Checkpoint screening increasingly also occurs at remote locations from the NextGen terminal to handle the increasing passenger and baggage loads. (See Secure Airport Remote Terminal Screening Site [RTSS]) for facilities related to remote screening of passengers and their baggage.) Passengers and luggage undergo screening at these remote locations and board transportation bound for the airport's sterile boarding area. The remote screening facility and the allocated mode of surface transportation are part of the sterile area. Screening at these locations is identical to that at the airport.

### **3.5 CONTINUOUS SURVEILLANCE AT CHECKPOINT/ACCESS SITES**

The continuous surveillance of people within the public areas of the airport is discussed in Secure Airports (Section 4). This section is restricted to surveillance systems and procedures at airport checkpoints and access and exit sites. Video analysis tools are able to automatically detect anomalies with bags and people. Video analytics may also be used to detect behavioral anomalies (behavior pattern recognition [BPR]) and/or undesirable events and to provide additional data for correlating with suspect carry-on and checked baggage or interactions with other people in the checkpoint or sterile areas (e.g., co-conspirators).

Beyond the security checkpoint, continuous security surveillance occurs at the gates within the aircraft. Video analysis tools are integrated with passenger information systems to provide alerts

for anomalous behaviors or events. For instance, the surveillance system can recognize in automated manner certain atypical behaviors associated with elevated risk (e.g., BPR).

### **3.6 GLOBAL HARMONIZATION**

The NextGen is committed to the efficient and safe movement of all air travelers to ensure security while promoting national competitiveness. The SSP is intimately involved with international bodies to minimize inbound travel of possible terrorists by use of globally harmonized screening activities. The SSP specifically benefits from joint development and investment from the international community to promote unified objectives for layered, adaptive aviation security for passenger prescreening programs. The SSP aviation security programs address international requirements for all aspects of secure people capabilities and appropriate related airport and aircraft activities.

## 4 SECURE AIRPORTS

The NextGen Airport (see Chapter 3) has an integrated facility security system scalable to differing capacity, access, and risk environments while maintaining the required NextGen standards. The Secure Airport ConOps includes technological and procedural measures to protect against the dynamically evolving threat. This flexible security system leverages advanced network-centric capabilities inherent in the NextGen to minimize redundant credentialing and access controls while providing shared situational awareness when security incidents occur or credentialing concerns surface.

The NextGen airport NEO seamlessly links sensors and data sources from access and screening checkpoints for passengers, visitors, employees and vehicles, perimeters, and critical facility infrastructure. The airport security technologies and adjustable procedures are nominally transparent to passengers and cargo, but difficult to exactly predict by those who intend harm. In addition, the NextGen airport has resident response and recovery programs enabled through local and regional memorandums of agreements (MOA) and supported by the US Government (USG). In this connection, the net-centric operations of the NextGen maintain real-time connectivity to other regional airport operators, law enforcement and USG intelligence and SSP operational entities. These tools enable quick ramp-up response operations to incidents of national significance, including CBRNE attacks on the airport or within the region. The emergency response has been appropriately gamed and rehearsed to ensure the responders are fully prepared for any contingency.

The layered and overlapping security systems are in place at the following types of airport facilities:

- Commercial (passenger/cargo) airports
- RTSS facility
- General (public and private) aviation airports
- Commercial spaceports.

They also are in place in the following areas within these facilities as appropriate:

- **Airside:** Security identification display area (SIDA)/AoA, terminal perimeter, terminal airspace (security)
- **Landside:** Terminal public and commercial roadways and parking lots, terminal entry and Departure, airline ticketing kiosk/counter, sterile area, international arrivals/customs, SCC, response and recovery operations

### 4.1 IRM—SECURE AIRPORT

IRM—Secure Airport prioritization strategies to enhance the robustness of airport security selected for implementation include an appropriate mix of people, procedures, infrastructure, and technology specific to the alternatives analyses and the countermeasures analyses. Similar to IRM—Secure People, technology investment is only one piece in the overall risk management of airports and is balanced with policy and procedures. (See Secure Airports, Section 2.2.)

## 4.2 AIRPORT FACILITIES

### 4.2.1 Commercial (Passenger/Cargo) Airports

Similar to the commercial airports of 2006, the NextGen Commercial Airport has scheduled passenger and cargo operations. However, a greater range of aircraft types (e.g., vertical takeoff and landing [VTOL], VLJs, super wide body, and UAS platforms) can cooperate at the same airport. The NextGen airport facility security consists of layered defensive systems designed to capture threat information on passengers, baggage, cargo, aircraft, and alert appropriate response. In addition, the facility infrastructure is hardened to better protect the public and aviation system employees from CBRNE threat objects used externally or internally on the facility.

### 4.2.2 Remote Terminal Security Screening

To facilitate the flow of passengers, baggage, and cargo, the SSP, airport authorities, and third-party approved security partners operate remote or offsite terminal check-in, security screening, and bag-check and screening facilities. A majority of RTSS serve super-density airfields to mitigate passenger movement demand and position initial security screening as far away from the terminal operations area as possible. The RTSS facilities are continually monitored and meet applicable security standards, whether fixed or transportable. Secure transportation services for passengers, baggage, and cargo are provided between the RTSS and the airport-secured transfer area designated for those categories. The transportable RTSS can be deployed during stress periods of traffic demand (e.g., special events) or in response to a National Significant Security Event. The technologies used (CBRNE sensors and weapons detectors), which are operated by the airport owner, USG, or a third party, are fully compliant with existing security regulations and standards. To the degree practicable, all luggage other than carry-on will be processed at curbside or off airport so as to not enter the terminal portal with the passenger-owners. Checked baggage will be processed remotely to the terminal passenger area.

Specialized RTSS are used to screen airline supplies destined for use on an aircraft for CBRNE threat. As described in the Secure Cargo and Secure People sections of this chapter there are also credentialing and secure custody chain requirements for these on-board supplies.

### 4.2.3 General Aviation Airports

GA airports in the NextGen can employ an SSP-approved security system scaled to the operational load and available infrastructure to achieve a lower facility risk profile. The security status and assessed risk of the GA airport is determined largely by the nature of the infrastructure present (including access controls), whether the airport is attended or unattended, and the type and quantity of aircraft operating there. Some GA facilities have a defined perimeter as with commercial airports; however, the level of sensor usage varies based on the size and type of aircraft operating at the airport and the proximity to high-risk metropolitan areas, sensitive restricted airspace or other special factors. GA airports that do not have an approved security system essentially operate as they did before the NextGen. Low-performance aircraft in the most cases are not significantly affected by higher facility risk profiles. However, higher performance aircraft or those aircraft capable of transporting a significant payload may experience an increase in their own flight object risk profile when they fly in more sensitive security areas.

#### **4.2.4 Commercial Spaceports**

The NextGen spaceport has security systems in place that have substantial overlap with other NextGen airports. However, some specialized features are required (e.g., access controls, credential verification, perimeter defense) as a result of the increased risk aspect of spacecraft systems, hazardous materials (fuel storage), and special launch and landing areas. The spaceport net-centric operations have secure access to the SSP and DSP, validating hypersonic aircraft clearances as they reenter the atmosphere to land at that facility.

### **4.3 AIRSIDE**

#### **4.3.1 AOA/SIDA**

NextGen Commercial Airports use various credential verification, access control, and surveillance systems to safeguard the aircraft, fuel farms, and other sensitive terminal airside areas, based on assessed risk and random measures. These include aircraft surface movement tracking, authorized vehicles-only screening, employee tracking, vehicle and employee access control (e.g., biometric readers and other advanced employee credential verification systems), unauthorized sector entry alerts based on credential status/level, vehicle and transportation worker tracking and identification, CCTV (daylight/infrared [IR]) on ramp areas adjacent to the airframe and occasionally airborne surveillance systems (i.e., UAS) to detect and track threats. The sensor and credential verification data are transmitted to the airport SCC (GA airports may have an NEI link to only a nearby SCC) as part of the airport net-centric operations, preanalyzed by NextGen decision support software applications and displayed in a usable form for incident response and interdiction. This capability is guided by a continual update of the employee status via NEO applications and the IRM, ensuring that any change in risk status is updated at the required latency. An important feature of this capability is the tracking of noncooperative targets (persons with no identification [ID]) that surreptitiously enter the AOA and alerting them of an appropriate law enforcement response via the SCC.

#### **4.3.2 Terminal Perimeter**

The NextGen airport perimeter is protected in various ways that may or may not include physical fencing. Depending on assessed risk and the practical and safety requirements of the airport site and surroundings, sensors, access control systems (ACS), closed-circuit television (CCTV), patrols, or other procedures with local LEO might be used. Where required or otherwise available, sensor arrays tied to existing ground surveillance radar can detect movement through the perimeter and alert (a) CCTV nearby to acquire the target and send unmanned ground vehicles (UGV) and/or (b) UAS systems to track and monitor the target until it is cleared or stopped. Adjacent stakeholders are intimately involved in maintenance of the perimeter, including fixed base operators (FBO) and air cargo operators. (Each operation offers distinct opportunities for unauthorized entry through its portals and shall be considered independently in this ConOps.) Airport law enforcement manages and operates this system, with data fed directly into the airport SCC via the NextGen net-centric operations.

### 4.3.3 Terminal Airspace Security

Where indicated by risk assessment as essential, a set of new ground-based defense systems can be deployed to protect the terminal airspace. These systems' operations are guided by the available information from net-centric connectivity to ANSP (e.g., Automatic Dependent Surveillance-Broadcast (ADS-B), Communications, Navigation, and Surveillance [CNS]) and UAS. These UAS systems have very small (nanotechnology) airframes that can be simply and cost effectively deployed around the community surrounding the airport and programmed to detect and defeat potential MANPAD activity, airport perimeter breach, or other suspect activity. The data received from the UAS systems are transmitted NEO, assessed, and acted on in the SCC.

## 4.4 LANDSIDE

Airport-related infrastructure redesign or modifications are guided by the *Recommended Security Guidelines for Airport Planning, Design and Construction* as a baseline. NextGen terminal security operations and potentially airport-related infrastructure (e.g., check-in, security screening, and bag-check/screening) are extended to remote and/or portable offsite terminal sites to better distribute initial security screening workload and increase throughput. Airport roadways, parking lots, and approach corridors are better protected with standoff CBRNE detectors and vehicle identification and tracking where required by risk assessment. Sensors for trace and radiated CBRNE and for operational procedures monitor public access areas of the airport terminal and sensitive facilities. ACSs for persons and vehicles and facility surveillance networks with NEO integration provide security in airside and vendor supply areas. The airport SCC, co-located in the onsite airport operations center (AOC), enables the real-time update of threat information and monitoring of airport operations and supports dynamic adjustments security layers based on risk assessments and intelligence.

### 4.4.1 Airport Public and Commercial Roadways and Parking Lots

A continuing threat to the NextGen airport is the vehicle-borne improvised explosive device (VBIED) or unconventional weapons of mass destruction (WMD). This threat is addressed through sensor arrays, CCTV anomaly detection, operational procedures, and other systems to detect threat vehicles before they gain entry or proximity to critical infrastructure. The airport LEO can activate installed recessed roadway barriers to manage vehicle access routes. Improved BPR techniques and decision support systems are employed by law enforcement officers and other trained personnel to identify individuals who might warrant closer scrutiny and possible intervention. The sensor data feeds directly into an airport SCC (shared regionally and nationally under the NextGen NEO as events dictate), transmits directly to handheld devices carried by law enforcement, and automatically directs police to intercept threat vehicles. Portable blast containment devices and reinforced shrouds are easily placed around the threat vehicle and provide enhanced blast mitigation or contain a CBRN threat.

### 4.4.2 Terminal Departures Curb

The terminal curb, which is the first point of contact with the physical facility, is monitored through CCTV systems able to detect anomalies in passenger behavior, vehicle size and weight,

and loiter time of vehicles. The security systems at the curb are similar to those described in the preceding section on public roadways, although the systems can be refined for closer proximity detection and mitigation. Sensor systems detect trace or radiated CBRNE from a standoff position and alert to potential threat. Sensors are managed and monitored by the airport or third-party, and airport law enforcement is responsible for policing the area and emergency response.

#### **4.4.3 Terminal Entry Portal**

The NextGen airport has terminal CBRNE sensors that are positioned within public access areas (curbside doors and entryways) to guard against threat devices entering the facility infrastructure. Air samples can be obtained to alert to CBRNE threats and provide preliminary location and identification information to response and recovery personnel through NEO. BPR continues to be employed by authorized personnel assisted by decision support tools to provide another layer of defense to public access areas.

#### **4.4.4 Airline Ticketing Kiosk/Counter**

Although a significant and increasing proportion of ticketing and baggage transfers are conducted at RTSS (off the airport property or on site, but not in the main terminal), this function is still present to some degree at the airport. The airport security systems and procedures used in public access areas also apply to the ticket kiosk or manned counter.

#### **4.4.5 Security Checkpoint**

Design of airport security checkpoints is integrated with overall terminal design to facilitate the flow of passengers and commerce. The checkpoint is integrated through the airport SCC to the NextGen NEO to enable more rapid and effective LEO response. The SSP uses the information to check for correlations with security incidents in other parts of the NextGen that may signal an unfolding security event. The security checkpoint exit lane in NextGen makes use of airport CCTV/person recognition systems that can acquire individuals proceeding the wrong way through an exit lane, visually lock onto the image, and track the perpetrator when nearing critical areas (e.g., gates, employee entrances).

#### **4.4.6 Sterile Concourse**

In the sterile areas of the concourse, facility sensors remain active to detect any threats, and LEO BPR are in place to capture CBRNE and conventional threats carried by passengers. CCTV systems transmit data to programs capable of detecting anomalies (BPR) in passenger behavior, and tracking passengers of interest, such as a passenger attempting to breach the checkpoint. These systems are linked to NEO communications systems at the airport and transmit information to law enforcement, guiding the response to enable the LEO to intercept the threat.

#### **4.4.7 International Arrival/Customs**

Airport security systems for sterile and public access areas are used. The security systems used by the US Customs Service, while technically outside NextGen, have been harmonized with the NextGen Airport security systems. This harmonization includes reducing incompatibilities and

redundancies of screening systems and providing connections between US Customs operations and the NextGen through the Airport SCC and NextGen NEO.

#### **4.4.8 Airport Concessions, Food, and Beverage Security**

Supplies intended for use at the airport public areas rather than transport on aircraft are handled through verified shipper and known source programs described in Secure Cargo. CBRNE screening is conducted when justified by risk assessment and for supplies not following Secure Cargo and Secure People requirements for the vendor supplies and personnel. Supplies intended for use in the sterile area have to undergo the procedures specified in Secure Cargo (Section 6).

### **4.5 AIRPORT SECURITY CONTROL CENTER**

The SCC is a facility operated by an airport operator that fuses all surveillance and data input associated with that airport. Principally operated by a combination of law enforcement and airport operations personnel, its staffing and infrastructure levels coincide with the size of the facility and operation. The ACC is the main connection point between the airport security system and the SSP and its security operations centers, as well as other SCCs as required. Note that this does not imply a single connection point to the airport because the NextGen NEO has built-in redundant pathways for information flows. (The airport's ability to detect, prevent, respond to terrorist attacks, and recover in a way that maintains continuity of operations depends heavily on the flow of surveillance, indicators and warnings (intelligence), and operational control messaging.) The SCC uses extensive and task specific data mining, predecision analysis and decision support software applications to reduce the amount of irrelevant information while increasing the quality of incidents requiring at least identification, if not outright response by airport, LEO, or SSP personnel. The SCC provides early warning to the airport operators, necessary telemetry data to guide response decisions, and accurate and timely information on incident aftermath to enable effective contingency response and continuity of operations.

### **4.6 EMERGENCY RESPONSE AND RECOVERY**

Through command and control systems operated by NextGen SSP, DSP and NEO, and through better defined policies and MOA involving first responders owned by various organizations and governmental agencies, the airport can quickly respond to a terrorist attack, security breach, criminal act, or disaster at the facility with the goal of saving lives, mitigating property loss, and containing the threat. The plans are routinely exercised to address CBRNE events and the airport maintains necessary staff and equipment for the initial response. Regional emergency management agencies, through the SSP or other authorized organization, can train and equip their staff to effectively respond to CBRNE attacks.

## 5 SECURE CHECKED BAGGAGE

The objective of secure checked baggage is to prevent checked baggage from endangering aircraft, aviation facilities, or people and from being used as a threat vector for the transport of CBRNE. Policy, procedures, and IT are combined to create the most effective system to accurately differentiate threats from normal commerce. Checked baggage screening equipment and sensors, with multisensor capabilities, are linked through secured NEO to the SSP and to LEOs and first responders. Between transfer into the NextGen baggage handling system and transfer out, services exist to identify and track checked baggage with tracking devices and related technologies and maintain link to passengers and boarding status information.

### 5.1 INTEGRATED RISK MANAGEMENT

The checked baggage screening system's capabilities respond to the risk profile and threat situation that IRM provides (e.g., higher alert state, special events, high risk airports) with different measures—for example, airports could change screening procedures, modify the sensor detection threshold, increase and decrease of random secondary screening, and deploy more security screeners or other personnel. The strengths and weaknesses of the devices and technologies determine the role each plays in the overall civil aviation security explosives detection mission. Identifying these roles ensures that investment decisions are appropriately made. Some considerations in placing CBRNE detector systems are those that are purely technical in nature, such as performance against threat types, bag throughput rate, and automation problems. Some nontechnical considerations are procurement and operational costs, system installation practicalities, public acceptance, and reliability and maintainability. For example, a decision regarding the inappropriate use of coherent x-ray scattering devices for 100-percent screening of checked baggage because of bag throughput limitations should not cloud an investment decision to use that technology in other more specific and pertinent detection schemes.

Airport threat classifications are reviewed periodically and changes in status call for detection equipment adjustments. Airport vulnerability analyses include CBRNE detector system deployment considerations consistent with the overall CBRNE detector system ConOps, individually tailored to fit that particular airport's needs. For instance, consistent with vulnerability analyses, equipment combinations responding to individual airports' needs can be identified airport by airport and managed, kept in proper working order, and supported on that basis rather than on an airline-by-airline basis. Equipment would then be rearranged or departure gates changed, depending on daily protection needs. The process leads occasionally to considerable changes in airport passenger flow and resultant terminal designs. (See Chapter 3, Airport Operations.)

IRM-secure checked baggage also takes advantage of NEO to adjust baggage screening based on risk. Before a flight's departure (upon reservation submission), IRM-secure checked baggage receives passenger data to assess overall NextGen security risk profile and, in turn, uses the IRM's alerting capability to share this risk information with all stakeholders through NextGen NEO. The stakeholders can respond and adapt to varying threat situations. Passenger prescreening using the integrated watch list identifies those items of checked baggage requiring additional screening. (See Section 2, Secure Checked Baggage.)

## 5.2 CHECKED BAGGAGE SCREENING

The NextGen checked baggage screening process, although having a significant correspondence with the baggage screening process instituted immediately after the attacks on 9/11, has incorporated several innovations that permit greater adaptability and flexibility with an expanded range of threat detection: a) sensor fusion for the full range of CBRNE threats, b) footprint reduction, c) reconfigurable or integrated systems for easy deployment, and d) NEI connections providing complete integration with NextGen NEO.

The basic process for checked baggage screening functions is as follows:

- Checked baggage screening
- Alarm resolution screening
- Threat object control procedures.

### 5.2.1 Screening

All checked bags undergo screening before being loaded on the airplane. This concept is in effect at all domestic airports. This identical technique or a screening technique determined to be equivalent is required at all international last point of departure (LPD) airports for us air carriers.

First-level (initial) baggage screening is designed to meet requirements defined by legal mandate to detect CBRNE threat amounts, types, and configurations. The need to integrate competing technologies arises from the complexity of the threat. CBRNE detectors can be deployed as one-box or multistage systems combination/integration devices depending on the site. A remotely based operator/analyst (with certain technical assistance from proximally located baggage handling and troubleshooting staff) analyzes machine nonresolvable alarms and expedites security response, passenger notification, or additional screening when required. Many routine decisions and alternate tests to screen suspect threats are performed by the installed hardware and software systems in automated manner. However, the screening system's effectiveness is ultimately determined by the human operators/analysts' ability to resolve expeditiously what has been detected by system components.

Bags that are cleared for loading aboard the airplane are segregated by carrier and flight, held in a sterile secure holding area, and loaded aboard the airplane. (See Security Sensitive Information Annex for additional details.)

### 5.2.2 Alarm Resolution Screening

The resolution of "alarm" bags depends on the nature of the alarm, contextual information related to the alert level, flight risk status, the passenger, and other similar alarms concurrently occurring in the SSP baggage screening system. Obviously, differing implications for the various classes of threats-suspected nuclear and chemical/biological threat objects would require the most elaborate caution because of their capacity to contaminate significant areas of the facility and surroundings. Policies, procedures, and integrated technologies are in place to handle these various circumstances. RFID or equivalent tags are attached to each piece of checked luggage to facilitate tracking in the airport and on the airplane and substantiate ownership. Note that one

benefit of sensor fusion is the opportunity to perform confirmatory tests on a suspected threat object. The confirmatory tests, which are by different kinds of sensors, have the inestimable value of providing an independent assessment of the initial alarm. If sensor fusion and technical advances permit, these overlapping tests can be performed concurrently. If not, then they can be sequential and contingency based. (See SSI Annex for additional details.)

### **5.2.3 Threat Object Disposal**

Policies, procedures, and technologies are available for the containment and disposition of bags determined to contain threat objects or materials. Where appropriate, threat objects are deactivated or otherwise made inoperative or detonated by explosives defeat systems. As a result of increased accuracy and specificity of the detection systems, the effect on airport operations can be better calibrated to the event and threat. Through NEO, the NextGen has shared situational awareness for these events and can adapt more quickly and economically to them. For example, flights may be able to land at a different concourses rather than diverting to another airport. In other more serious circumstances, flights may divert to a close alternate airport and when the plane arrives, local transportation is already there to ferry passengers and baggage.

## **5.3 CHECKED BAGGAGE SCREENING INSTALLATIONS**

The differing environments in which baggage screening takes place put constraints on the CBRNE detector systems. These constraints can be physical limitations or ergonomic and policy considerations. Physical limitations include the amount of available space or strength of the floor in the building in which the system is to be deployed. Ergonomic considerations include noise level, processing time of a passenger bag, baggage handling requirements, ease of maintenance, and safety and health hazards. Policy considerations include the total cost of the system, including maintenance and personnel training for operators and inspectors.

However, the greater variety of detection equipment that can be deployed in the NextGen permits customized installations by airports' threat classifications. Those with high threat vulnerability profiles would receive different combinations of equipment from those with low-threat vulnerability profiles. Similarly, screening locations with specialized or intermittent baggage screening have correspondingly tailored CBRNE detector deployments.

### **5.3.1 In-Line Baggage Screening**

The NextGen uses in-line baggage screening installation at airports with high levels of enplanements. This action greatly enhances throughput, even with super-density operations. Checked baggage undergoes screening in the airport's baggage makeup area for the in-line system. Checked baggage is delivered to the baggage makeup area from the check-in counter by an automated baggage transport conveyor system to one or more CBRNE detections systems. After screening, bags that trigger an alarm are subject to alarm-clearing procedures and technologies.

### 5.3.2 Nonintegrated and Standalone Baggage Screening

Non-inline CBRNE detection system installations occur in airports and other screening locations that lack high throughput demands or where inline systems installations are not feasible for other reasons. They are designed as rapid deployable units for low-capacity demand and temporary and intermittent screening locations, and they can be deployed preintegrated with other airport customer service functions. These systems have either an automated baggage loading and unloading interface or a manual interface that is ergonomically designed to minimize safety and health hazards. With these systems, procedures are in place to ensure the chain of custody of screened baggage to the aircraft.

### 5.3.3 Deployable Baggage Screening Operations

Remote screening of checked baggage also occurs at locations away from the airport terminal building to handle the increasing passenger and baggage loads. Passengers and luggage undergo screening at these remote locations, and board transportation bound for the sterile boarding area at the airport. The remote screening facility and the transportation media are part of the sterile area. Screening at these locations is identical to that at the airport.

Occasionally, the baggage screening systems are an integrated part of a deployable airport infrastructure component. These deployable units service smaller capacity or intermittent service airports that do not have a business case for supporting a large-scale or permanent infrastructure to handle security functions and might also incorporate other airport customer services. (See Chapter 3, Airport Operations.)

## 5.4 GLOBAL HARMONIZATION

The SSP is intimately involved with international aviation organizations to minimize inbound checked baggage containing unauthorized CBRNE through the use of globally harmonized screening activities. The SSP aviation security programs for screening checked baggage have sought maximum adherence to the required standards without mandating a particular technology or process to achieve that standard. Countries meeting these standards benefit from expedited processing of checked baggage by avoiding redundant screening operations. The SSP offers consultative services as well as excess equipment transfers to facilitate the adoption and maintenance of baggage screening requirements in foreign airports with direct flights to the NAS.

## 6 SECURE CARGO AND MAIL

Cargo represents a critical vulnerability that was addressed historically mainly through the deterrence value of background investigations, inspections, and paper trails required of shippers, both known and unknown. The NextGen vision for cargo security moves beyond that to also include freight vulnerability assessments (through the IRM process), identifying the risk level of cargo, use of sterile area cargo packing areas, cargo transit safety and integrity, and CBRNE screening for air cargo.

Secure cargo/mail has the objectives to prevent not only checked cargo and mail from endangering aircraft, aviation facilities, or people but also the air cargo system from being used as a threat vector. These objectives are met using a combination of policy, procedures, and IT to accurately differentiate normal commerce from threats. Cargo and mail screening equipment and container sensors, with multisensor capabilities, are linked through secured NEO to the SSP SOC and other analysis centers.

The security of cargo and mail begins at the point of initial packing (or when that is uncontrolled, initial screening) with either the manufacturer, freight consolidator, air carrier, or licensed US customs broker. The SSP integrates all information related to the flight, cargo, and aircrew to provide additional information and ensure security during transit, enabled through NEO. It includes the following concepts:

- Vetting for secure supply chain entity (SSCE)
- Vetting for certified supply chain entity (CSCE)
- Security screening
- Loading and storage security
- Surface transportation security/tracking
- Cradle to grave tracking/integrity.

The air cargo supply chain has many potential organizations and personnel involved in the transport of any given piece of cargo: a source or shipper, freight forwarders, indirect air carriers, and other commercial and government personnel. Because of the many potential transfer points, cargo and mail security have to take into account the entire custody chain. A continuous risk and threat assessment must be conducted to identify risks to the supply chain; assess those risks; and apply measures, procedures, and policy to reduce those risks to an acceptable level. A secure supply chain encompasses the concept that cargo must be initially packed in a sterile area and conveyed through a secure chain or custody to the aircraft. If any deviance from this process occurs, all cargo intended for air transport whether on passenger flights or all-cargo operations must undergo CBRNE screening from either the SSP or a CSCE. After CBRNE screening, the integrity of the goods shipped must be maintained until the cargo exits the air transportation system. SSCE and CSCE are regularly inspected for compliance. All personnel with access to shipped goods must be properly screened and trained to ensure a secure shipping environment. In addition, all cargo items are subject to random inspection and CBRNE screening to maintain necessary variability and verification of the supply chain.

## 6.1 INTEGRATED RISK MANAGEMENT

Before a flight's departure, IRM-Secure Cargo capability receives cargo, shipping, and other threat data to assess overall NextGen security risk profile and, in turn, alerts the stakeholders concerning potential risks (e.g., higher alert state, special events, high-risk airports, types of cargo). Such information sharing is through the NextGen NEO. The stakeholders can thus respond and adapt to varying threat situations by having improved situational awareness. The cargo screening system capabilities respond to the risk profile and threat situation that IRM provides with different measures; for example, airports could change screening procedures, modify the sensor detection threshold, increase and decrease random secondary screening, or deploy additional security screeners or other personnel. A freight assessment threat management system evaluates specific information about shippers (e.g., the environment at the shipment origin and the individual or personnel processing and packing it) and the goods they ship (e.g., the physical and logistical difficulty of screening the items or the detectability of inserted threats) and assigns corresponding risk scores that determine screening methods and air transportation constraints.

IRM uses NextGen-unified NEO capability to notify all relevant stakeholders through NEO so mitigation strategies can be coordinated and implemented, and relevant operational data can be fed back to IRM—Secure Cargo. (See Section 2, Secure Cargo/Mail.)

## 6.2 SHIPPER CREDENTIALING

The NextGen security system for air cargo, with risk profiles rated in excess of a defined threshold, uses a tiered certification process offering certifications for SSCE and CSCE status based on various levels of screening capability, cargo integrity technologies, and other NextGen credentialing processes. (Note that the risk profile mentioned here is for the cargo item itself, not the flight object. See para D.6.3 for flight object risk and cargo.) Applications to join the SSCE and CSCE programs are vetted against terrorist and law enforcement databases. When assessing an application to join the SSCE or CSCE program, the SSP evaluates the character, reliability, and susceptibility to compromise the persons involved. Airlines operating under an all cargo security programs should accept cargo from only a shipper with an SSP-approved security program unless they have their own cargo screening operations.

The Secure Supply Chain Entity Management System integrates shipper credentialing and regulated shipper-controlled security inspection processes to reach cargo security compliance targets while minimizing impact on commerce. The SSCE is responsible for enforcement of all regulations in the segments of cargo preparation, transport, and receipt it directly controls within a trusted and monitored chain of custody. Essentially, they must maintain and control a sterile environment for initial cargo item packing in accordance with approved specifications and configurations coupled with the direct (nonpaper based) verification of the containerization (e.g., video records). Conveyance to the aircraft must be successfully completed through an approved SSCE or the cargo are subjected to CBRNE screening, unpacking or rejected for air transport. CSCEs also have the verified capability to perform nonintrusive technology-based CBRNE screening for some or all of their cargo shipment to expedite handling.

## 6.3 SCREENING AND INSPECTION

All air cargo associated with flight object risk profiles above a defined threshold and not meeting SSCE sterile area packing and chain of custody requirements are screened for CBRNE threats (mainly through specialized screening systems) before loading on an aircraft. Cargo screening can be conducted as early in the supply chain as a secure method of conveying it to the aircraft can be maintained. Cargo screening equipment typically accommodates standardized industry practices related to the movement of goods. The NextGen cargo screening process permits airport and offsite cargo screening facilities by CSCEs to ensure the free flow of commerce. If screened off site, the secure cargo supply chain ensures the integrity of the screened goods during transport to the air carrier. All persons who receive, inspect, transport, or load air cargo, or who have unescorted access to air cargo or all cargo aircraft have been vetted using relevant data bases or credentialed, as appropriate.

To detect CBRNE agents and other threat materials, NextGen cargo security uses sensor technologies designed specifically for inspection of cargo intended for air transport by Direct Air Carriers. These systems deliver improved performance in throughput, threat detection, maintainability, ease of installation, and reduced false positives. A small proportion of cargo intended for air transport may not be capable of being screened effectively for all threats even with NextGen technology. These would need to be packed in accordance with SSCE sterile area requirements for cargo packing. Other procedures must be used in such circumstances through the SSCE and CSCE programs. For example, a CSCE source would verify a container's contents through a video record of the initial packing and, where required, with their own screening of the individual unpacked items. The package would be placed in a tamper-proof container and transported through secure ground transportation to the airport. An alternate approach would be to use an acceptable form of IED Defeat Technology to achieve the 100-percent inspection requirement.

For the most part, pre-NextGen acceptance sites remain operational if useful, provided that cargo integrity can be maintained. However, NextGen has additional acceptance and cargo screening sites to improve the flow of commerce.

## 6.4 ALARM RESOLUTION

The resolution of "alarm" cargo containers depends on the nature of the alarm, contextual information related to the alert level, the shipper/source, and other similar alarms concurrently occurring in the SSP baggage screening system. Many of the same considerations apply as with checked baggage (see Section 5.2). The major differences are the relative inaccessibility of the shipper compared with the passenger and the general difficulty in opening cargo containers for inspection. Therefore, not every piece of intended air cargo is loaded onto an aircraft, although a vast majority do. For cargo items known to be difficult to screen, it is incumbent on shippers requiring air transport to adopt other approved means to verify their cargo, as in the example above. (See SSI Annex for additional details.)

## **6.5 SURFACE TRANSPORTATION SECURITY OF SCREENED CARGO**

Cargo screened before arrival at the air cargo facility on airport is surrounded by a “chain of custody” umbrella providing NEO-linked tracking and protection, from origin (i.e., initial screening point) to the airport in a secure environment (e.g., truck), which is sealed and tamper-proof. Cleared unit load devices (ULD) are locked with tamper-proof seals and devices. Access controls for persons and vehicles are implemented on all cargo ramps that are the same or equivalent to SIDA requirements. (See Section 3, Secure People, and 4, Secure Airports.) All persons who screen, transport (after screening), load cargo onto the aircraft, or who have unescorted access to air cargo or all cargo aircraft, have credentials and receive authentication at access points.

## **6.6 HARDENED DOORS AND BARRIERS ON ALL CARGO AIRCRAFT**

NextGen air cargo airliners have a special barrier between the cockpit and cargo areas to prevent persons in the cargo area from attacking the crew unawares. The barrier is sufficient to give the crew time to take necessary actions in response to the threat and signal the emergency. (See Section 8, Secure Aircraft.)

## **6.7 SECURITY TRAINING FOR ALL CARGO FLIGHT CREW AND STAFF**

All cargo flight crews receive the same security training as passenger flight crews. This training includes Crew Member Self-Defense Program, Federal Flight Deck Officer training and BPR training, and access to pertinent SSP Security Directives and Information Circulars (see Section 8, Secure Aircraft). This also includes training in recognizing cargo that may have been tampered with.

## **6.8 STORAGE SECURITY**

Once the cargo has been screened and cleared for shipment, the cargo remains in a sterile isolation, secured and protected until it reaches the aircraft cargo hold (at origination and staging areas on airport). These measures include physical security and application of technology to produce virtual barriers around the sterile area, capable of alerting any unauthorized entry.

## **6.9 CARGO TRACKING AND INTEGRITY**

Throughout the transport process, the air cargo is tracked and monitored until it reaches its destination, again using NEO capabilities. Cargo is placed in containers with sensors/devices, which provide proof of tampering. For those cargo items or shipments identified by risk management as security risks if stolen/diverted, tracking, diversion, or other identification data is provided through NEO to the SSP.

## **6.10 GLOBAL HARMONIZATION**

The SSP is intimately involved with international aviation organizations to prevent the shipping of unauthorized CBRNE materials to the United States through aircraft. The SSP aviation security programs for cargo tracking, screening, integrity, and screening have sought maximum

adherence to required standards without mandating a particular technology or process to achieve that standard. Countries that meet these standards benefit from expedited processing of cargo by avoiding redundant screening operations. The SSP offers consultative services and excess equipment transfers to facilitate the adoption and maintenance of cargo-screening requirements in foreign airports with direct flights to the NAS.

## 7 SECURE AIRSPACE

The major objective for secure airspace is to prevent or counter external attacks on aircraft and other airborne vehicles anywhere in the NAS or to use an aircraft as a weapon to attack assets and events on the ground. To reduce the security risk within the Air Domain, NextGen Secure Airspace systems and procedures detect and prevent or mitigate: a) anomalies in aircraft operation that indicate unauthorized use or attempted unauthorized use, b) aircraft not providing the appropriate cooperative data concerning identity and intentions, c) external attacks on aircraft, d) aircraft that can pose a threat from operating in the NAS. These risk management requirements include defining (usually dynamically) the boundaries of security-restricted airspace (SRA) and temporary flight restrictions (TFR), the cooperative division of responsibilities between the DSP and the SSP in the event of security events in flight or by airborne threat aircraft, security personnel on flights, and modifications and equipment to the aircraft. SRA and TFRs will be implemented as a last resort throughout the NextGen network, not as a routine procedure. In addition, secure airspace implements airspace access and flight procedures based on a verification process that dynamically adjusts for aircraft performance capabilities. The model combines credentialing data with performance data as part of developing the risk profile of the flight object. One objective is to permit increased NAS access by low-performance aircraft through most restricted zones because the reaction time to intercept is correspondingly greater than with high-performance aircraft.

### 7.1 INTEGRATED RISK MANAGEMENT

The IRM—Secure Airspace process (see Section 7.1) identifies locations of security interest and establishes the requirements for NAS protection from the four threats described above in Section 6. This risk management process requires close coordination between the ANSP and SSP and in some areas with the DSP. For example, the SSP uses the intelligence and threat information made available in the IRM process (see Section 5.1) to establish the operational requirements for the SRAs, time interval, size of airspace, and access criteria. Through collaboration with the ANSP and the DSP, the access criteria incorporate the criticality of the protected site or object, the aircraft performance specifications, and the verification level (credentials) of an operator crew, passengers, cargo) to determine the SRA size for a given flight object. For flight objects governed by flight plans, the ANSP can use the risk profile to formulate an appropriate four-dimensional trajectory (4DT). Consequently, lower risk flight objects in the NextGen experience fewer restrictions through SRAs. Even low-risk flights operating on visual flight rules (VFR) (such as low-performance aircraft) have increased access through the dynamically defined SRAs.

### 7.2 VERIFIED AIRSPACE ACCESS

Integrated airspace operations (see Section 7.1) provides a full discussion of the types of airspaces in NextGen ranging from those with general or universal access to highly restricted zones attributed to performance requirements or security considerations. As noted, the NextGen ATM service received by a flight depends on the aircraft's performance and equipment capabilities and its flight object risk profile. From the security perspective, the right to transit through non-universal access NextGen airspaces is based on a verification process that brings together relevant information for defining a flight object risk factor. Aircraft unverified on one or

more of the following risk factors is still able to operate in appropriate low-risk NextGen environments, but the lack of verification does affect their risk profile if they transit more restricted airspace. This method has the following summative verification and credentialing factors:

- Flight operator's security performance is certified based on SSP-issued requirements.
- Aircraft is registered, and its legacy has chain of custody integrity.
- Aircraft operator's identity is known and verified before flight becomes airborne.
- Crew and passengers have been credentialed before a flight becomes airborne (secure people capability).
- Aircraft content (e.g., baggage/cargo/mail) has been screened (secure checked baggage and secure cargo/mail capabilities).
- The aircraft has communication capability air to air and air to ground throughout flight to maintain verification status of identity and intentions.

In the NextGen, verified aircraft have access to the full set of authorized functions for their equipage. This does not mean that all aircraft must satisfy all aforementioned security requirements to have access to the NAS. As discussed in Chapter 2, standard VFR operations can still be conducted in specified airspaces. In addition, low risk-profile flight objects operating with VFR often may have an increased level of access through security zones compared with pre-NextGen NAS procedures.

### 7.3 SECURITY RESTRICTED AIRSPACES

SRA airspace is put in place to protect key assets and activities that are of national security significance. Their geometry, volume, and activation schedules are efficiently structured and implemented to balance security and air traffic demand. The use of SRAs for security purposes is kept to the minimum required to maintain security standards and maintains as much flexibility as possible to avoid impeding the flow of commerce. In addition, NextGen SRAs are no longer defined in terms of distance units but instead as time-based units (i.e., time to transit or reaction time to intercept). An SRA is segmented into the SRA minimum zone in which transiting aircraft are not permitted and one or more risk-level extension zones. Higher risk profile aircraft have to avoid the maximum SRA zone while those with lower risk profiles can cross closer to the SRA minimum.

If IRM—Secure Airspace identifies SRAs as a risk mitigation strategy to protect certain critical assets, locations, or activities, the NextGen secure airspace capability defines multiple alternatives for restricted airspace volumes and timeframes. This assessment leverages NextGen trajectory-based operations (TBO) capability to assess overall NAS impact based on projected demands. The “what-if” capability from TBO forms the analytic basis for determining the optimal SRA volume size, SRA minimum zone and extension zones, access criteria, and their associated security requirements and procedures.

In the NextGen, it is envisioned that the temporally defined SRAs have the following general types:

- Total restriction SRA (few locations)

- Airspace access is limited to only security and defense operations.
- No exemptions.
- Continuous restriction SRA
  - Airspace that has some security performance requirements to gain access.
  - Access exemptions are risk based.
- Intermittent restriction SRA
  - Airspace that has high-security performance requirements for certain time periods; the remainder of the time, no restrictions.
  - Access exemptions are risk based.

As noted, an SRA is based on the criticality of the protected site/object and the risk profile of the flight object and can be either permanent (e.g., the US Capitol) or short-term (e.g., nuclear materials transport at a power plant) for total restriction SRA. Continuous, but not total, restrictions SRA could apply to large metro areas that are major population centers. Intermittent restriction SRAs could apply to major sports or political events or locations that have large gathering of people for a limited timeframe. An exemptions process is available to handle special circumstance such as emergencies and activities that warrant special considerations (e.g., flights carrying foreign dignitaries). In addition, access to SRAs during severe weather conditions could also be a basis for exemption. The exemption process is conducted efficiently without incurring delay.

## 7.4 AIRSPACE VIOLATION DETECTION, ALERTING, AND MONITORING

The total flight monitoring capability in secure aircraft (see Section 8) calculates a security factor that is continuously being updated. In real time, the secure airspace capability receives data updating each flight's security factor. The separation management (SM) capability (Section 2.2.8) detects potential violations of SRAs from cooperative and non-cooperative flights within a look-ahead time. The detected airspace violation alert notifications are sent to operational personnel who have positive control responsibilities for the aircraft, including the flight operator and ANSP. Depending on aircraft type, the cockpit may also be equipped with airspace violation detection capabilities that could alert the flight operator directly.

The TSM automation proposes resolutions (e.g., reroute) to deconflict the airspace violations and the flight operator execute the resolution. Airspace violations are continuously monitored to ensure deconflict maneuvers are implemented. Alert status is escalated when the aircraft does not respond timely or take directed action to achieve authorized trajectories. If an airspace violation alert is not resolved in a timely manner, the NextGen SSP and DSP are notified. In addition to airspace violations, alerts concerning flight anomalies or behavior on board could be detected by the Federal Air Marshals Service (FAM), crew, or other LEOs and could potentially be reported through the following paths: FAMs/SSP and flight operator/ANSP. Such alerts are shared through the NextGen NEO with the DSP and other stakeholders.

The alert situation is continuously monitored by automation and by the ANSP and SSP personnel to determine when/whether the alert status has to be further escalated. The secure airspace has a set of criteria for alert escalation, for example,

- The same aircraft violates the restricted airspace multiple times.

- An aircraft does not change its flight profile to avoid or exit the unauthorized trajectory or airspace.
- An aircraft with an airspace violation has a security factor that exceeds the security threshold.
- Multiple unauthorized aircraft penetrate the same airspace simultaneously.
- Look-ahead time to point of (critical) violation is short.
- The aircraft fails to communicate with the ANSP repeatedly.
- Aberrant behavior on board is not resolved.

The secure airspace capability also does automated recordkeeping of violations of SRAs. Such data are used for pursuing follow-through actions for noncompliant aircraft operators.

## **7.5 INTEGRATED MANAGEMENT OF AIRSPACE SECURITY**

Response to airspace security incidents is time critical with many organizations that have to act simultaneously and/or sequentially. This response cycle of the incident management process is human-centered with automation providing information updates, situation monitoring, and decision support. NextGen IRM's unified C3 capability (see Section 2.3) provides the operational and communication infrastructure for notifying and facilitating collaboration with all relevant stakeholders, especially the ANSP/SSP/DSP, flight operator, and the flight operations center (FOC) through NEI so risk mitigation strategies can be developed, coordinated, and implemented. Through policy and standards development, NextGen has an integrated multiagency command structure with clear roles and responsibilities for decision-making, with one organizational entity at the lead position.

### **7.5.1 Non-Cooperative Surveillance**

In the NextGen, all aircraft above a certain size or flying in specified environments must broadcast identifying information and respond to predesignated queries. (All UASs without exception must do the same.) However, to preclude threat or other rogue aircraft from operating unannounced or surreptitiously in the NAS, the NextGen has a non-cooperative surveillance capability. (See Chapter 5, Non-Cooperative Surveillance.)

Upon detection of a non-cooperative aircraft, the SSP requests, through the ANSP, information on the flight. If the non-cooperative aircraft is not identified and cleared, the SSP initiates an alert to the appropriate SOC. Additional observation and data collection are initiated, which in critical circumstances may lead to DSP interdiction.

### **7.5.2 Countermeasures**

When an alert reaches a high-severity level, the alert becomes an incident that the SSP and ANSP have to develop counter measures to reduce the risk. There are two countermeasure alternatives: reroute/diversion and/or interdiction. Reroute/diversion strategies are developed with considerations of minimizing impact on other flights and on the overall NextGen system. When an incident occurs, the unified command center leads the coordination and monitoring of the development of the incident. The ANSP is the direct interface with the flight. Consequently,

while the incident is still being monitored and has not exceeded a risk threshold, the ANSP acts as the lead who consults with the SSP and DSP.

Interdiction is another countermeasure option. This option could be combined with reroute/diversion. The interdiction countermeasure is used in situations, especially when an aircraft fails repeatedly to communicate with the ANSP. The ANSP, in close coordination with the SSP, makes the decision to interdict and seeks military assistance from the DSP.

The DSP is responsible for providing the defense asset for interdiction. During interdiction, the defense provider continues to monitor the situation and coordinates decisions and actions with the NextGen combined operating command center. The DSP is in the lead during interdiction. It has a stringent set of engagement rules to ensure satisfactory interdiction outcome.

### **7.5.3 Joint Exercises**

Response to airspace security violations involves many stakeholders; therefore, NextGen has an infrastructure and a set of simulation and training capabilities that could facilitate joint exercises (war-gaming) among many stakeholders. Such an infrastructure delivers “virtual” violation events as part of security scenarios to validate the plan and procedures put in place for security violations coordination, monitoring, and countermeasure execution.

## **7.6 COUNTER PROJECTILES**

Projectiles, including MANPADS systems, are defined in the broadest sense here as any ground-launched projectile capable of bringing down an aircraft at altitudes from liftoff to 10,000 feet, including MANPADS, rocket-propelled grenades, anti-armor weapons, mortars, and other similar devices.

### **7.6.1 Airport AOA/Terminal Airspace**

Local and regional intelligence is considered in the IRM assessments of MANPADS attacks to determine rank-ordering, prioritization, and otherwise assess the MANPADS threat at airports. The analysis includes a site-specific analysis of MANPADS threat corridors adjacent to the airport, airport perimeter security, counter MANPADS systems in place, and joint operating procedures established with local and adjacent LEO jurisdictions and with the SSP, DSP, ANSP, and Department of Justice (DOJ). The product of this continually updated process is a priority of mainly ground-based counter MANPADS installation investments at vulnerable airports but with some aerial surveillance by UAS and other aircraft. The aerial surveillance is concentrated on vulnerable terminal airspace based on threat. This process has policy implications because these systems (e.g., UAS, UGV, other NextGen sensor systems) are costly and may not necessarily enable rapid installation. The assessment also directs local LEO jurisdictions to develop and implement operational programs that provide added surveillance and interdiction capability on the ground. This preflight phase addressing counter MANPADS terminal operations is conducted well before a particular flight. Infrastructure or other system installations extend the lead-time for this phase.

### **7.6.2 Aircraft/Flight Object**

Once a flight is planned, scheduled, or initiated, the IRM determined risk level is established for that flight or aircraft. The IRM information is tied to a flight object and continually updated with information obtained from the NextGen NEO until the flight concludes. Information relating to local or regional MANPADS threats can be assessed immediately via SSA links to local joint terrorist task forces (JTTF) and other LEO organizations. A threat spike of predetermined magnitude may direct the ANSP to affect a change in trajectory management (routing) or divert the flight object.

## 8 SECURE AIRCRAFT

Secure aircraft increases the safety and security of the NextGen aircraft in flight through various hardware, software, personnel, and procedural methods. The threats that require mitigation are hijacking and unauthorized diversion, internal explosive destruction, external attack, onboard CBRN or other attack of crew, passengers, or aircraft systems, aircraft use as a transport for CBRNE, and aircraft use as a WMD. Secure aircraft applies to civilian passenger aircraft and civilian cargo aircraft. UAS aircraft (surveillance or cargo) also is included for threats related to unauthorized diversion, internal explosive destruction, and as a transport for CBRNE.

### 8.1 INTEGRATED RISK MANAGEMENT

Continuous threat assessment and risk management processes identify all security-related vulnerabilities and risks associated with various types of aircraft and aircraft operations and scheduling in the air transportation system. Mitigation strategies and countermeasures for a given aircraft depend on risk assessment and threat/alert levels. Integrated decision-making through NEO increases decision quality and decrease response time to events.

### 8.2 AUTHORIZED CONTROL OF THE AIRCRAFT

Maintaining authorized control of the aircraft is the most essential and obvious step to preventing using aircraft as a WMD and to other hijacking/unauthorized diversions. (Note that the aircraft may either have a pilot/crew or be a UAS.) However, it also prevents or significantly mitigates the threat of aircraft cabin.

#### 8.2.1 Cockpit Systems

The NextGen aircraft assessed to be a significant risk for use as a WMD or hijacking diversion has certain aircraft hardware and software systems that the pilot or UAS controller can use to prevent unauthorized diversion or, at the least, provide a signal that the aircraft is no longer under authorized control through the ANSP to the SSP. (See Secure Airspace section for concept when control cannot be restored.) Special communication channels also are installed in such aircraft, which provide secure two-way data and voice transmission from cabin and cockpit to the DSP and SSP directly in the event of a critical security incident.

#### 8.2.2 Onboard Personnel

Although the NextGen aircraft is very well protected against the typical methods of hijack, there is still a need on certain higher risk flights for onboard LEO and other security-related personnel to guard against cabin takeovers, acts of malice (e.g., suicide bombers), or unexpected threat activities. To defend flight decks of passenger aircraft against acts of criminal violence and air piracy, personnel include specially trained flight deck crew, cabin crew staff, assigned on-board SSP personnel armed and operating clandestinely, and other armed LEOs traveling on that flight. To maintain shared situational awareness, SSP personnel have advanced communication systems that permit air-to-ground and air-to-air communication (and to the cockpit) with the ANSP, SSP and DSP. In addition, SSP personnel benefit from other NEO-based systems and programs that identify and leverage the presence of other armed LEOs as they travel on their routine business

(e.g., prisoner transport) on a given flight. This information aids in scheduling mission/flight assignments for SSP LEOs. Training and USG agreements with local LEO organizations allow nonfederal LEO to assist SSP on-board LEOs. (Additional information about on-board protection is available in an SSI annex to this report.)

### **8.3 AIRCRAFT MONITORING/SURVEILLANCE**

Surveillance sensors and CCTV are used to detect, monitor, and in certain cases mitigate cabin attack by passengers or by release of threat agents and aircraft use as a transport for CBRNE in at-risk aircraft. They also provide an additional data resource if hijacking/diversion of the aircraft occurs. Security sensors and surveillance are present in the flight deck, cabin, and cargo hold. The flight deck also contains the onboard control center for these systems, which is biometrically activated by authorized crew.

#### **8.3.1 Cockpit, Cabin, and Cargo Hold Surveillance**

To provide security personnel with a better understanding of the actual situation in a particular aircraft, a cockpit, cabin, and cargo hold surveillance (CCCHS) capability is incorporated in at-risk aircraft. The installed systems are completely integrated into the ANSP-provided communications and data network capabilities. They are lightweight, compact, and create no additional safety hazard to passengers, crew, or other aircraft systems. During security events, real-time video, with compression and time-limited segments, of the cockpit is compatible with flight data and voice recorder transmissions. The onboard SSP also can access security-related data streams from this system through handheld communication systems and can transmit portions of the data to the SSP SCC and SOC responsible for the flight. Thus, security personnel have a capability during security events to view in real-time the cockpit, cabin, and cargo hold surveillance videos.

#### **8.3.2 Continuous Air Monitoring**

Lightweight and safe continuous air monitoring (CAM) systems are installed in at-risk aircraft to mitigate or prevent release of CBRN threats in the cabin and cargo hold. They provide an additional security layer mitigating the use of the aircraft as a vector for transporting such threats by cargo, baggage, or by passengers themselves (e.g., bioterrorism or illness). To detect naturally occurring or criminally introduced chemical or biological (CB) threats in the cabin or cargo hold, small, lightweight advanced technology sensor systems are used in conjunction with robust NEO-based communications, installed without affecting safety. The CAM systems also have some proven crew/LEO ConOps that may be used to flush contaminated air from the cabin or otherwise mitigate effects, and/or automated air treatment capabilities so that certain airborne threats, primarily biological, can be neutralized or sterilized to protect cabin and crew during the flight. Indicators of potentially dangerous situations (e.g., heat and smoke detectors) are leveraged off aircraft safety systems. Procedures are in place to divert aircraft suspected of contamination to appropriate facilities within the United States that are able to safely treat passengers and decontaminate aircraft.

## 8.4 AIRCRAFT HARDENING AND DEFENSIVE SYSTEMS

Hardening the aircraft structure, internal systems/components, and/or accessory devices (e.g., cargo containers) can enhance aircraft security by mitigating internal explosive destruction and external attacks. Because of the expense, safety implications and difficulty of adding hardened systems to civilian aircraft, the SSP, DSP and ANSP form a collaborative research, development, test, and evaluation (RDT&E) effort to enable proof of concept, simulations and prototype development, and operational suitability assessments of various alternative designs. A particular requirement is the development of a low-cost and weight barrier to separate cargo aircraft flight decks from the cargo area.

The goal is to have several preapproved (flightworthiness certified) accessory devices or design changes for at-risk aircraft types that can be retrofitted and implemented if the security situation requires it. In all cases, the priority is to leverage ongoing safety modifications for concurrent mitigation of attacks.

One such example implemented in NextGen aircraft is the use of fuel and fuel tanks with enhanced resistance to explosion, while leveraging the ongoing nonexplosive fuel research. In addition to the obvious safety improvement, these approaches provide mitigation of projectile or directed energy attacks on an aircraft. New construction techniques and materials also help aircraft better tolerate internal explosions or external attacks. The overarching goal is to use the IRM model to develop high-return aircraft security enhancement and hardening elements for aircraft during airframe/system design, in lieu of retrofit design, significantly reducing cost implications.

For defensive systems, leveraging safety modifications to enhance the mitigation of external threats to the aircraft is the first priority. For those aircraft types assessed at risk, NextGen aircraft design standards identify and prioritize modifications to increase shielding of critical flight systems from direct energy weapons and electromagnetic pulse (EMP) technologies and events. Procedural and operational technique training for flight crew in response to MANPADS, laser and directed energy attack are standard for NextGen aircraft assessed at risk.

## 8.5 SAFETY INTEGRATION

Aircraft security solutions for NextGen (e.g., systems, equipment, procedures) undergo the safety risk analysis and management process prescribed by the NextGen safety management system (SMS). The NextGen safety management process specifies a collaborative and integrated safety and security hazard/threat mitigation strategy so the security threat mitigation and safety hazard mitigation could complement, and not conflict with, each other. (Also see Chapter 8, Safety Management Services).

## References

1. ASME Innovative Technologies Institute, LLC. *Risk Analysis and Management for Critical Asset Protection (RAMCAP) Applied to Terrorism and Homeland Security*. Version 1.1d, October 5, 2005.
2. *Recommended Security Guidelines for Airport Planning, Design and Construction* (TSA reference document). (Need complete references here.)
3. RMAP and RAMCAP Risk Management references.
4. 49 CFR Parts 1520, 1540, 1542, et al., *Air Cargo Security Requirements*. Final Rule, May 26, 2006.
5. *National Infrastructure Protection Plan*, 2006.